

## Artikel Boeing medewerker steelt info via USB stick

Door Redactie infosecurity.nl op vrijdag 10 augustus 2007 10:54

Het lekken van informatie is al tijden voorpagina nieuws. Zo werd onlangs nog een werknemer van Boeing aangeklaagd wegens het stelen van vertrouwelijke documenten die hij op een USB-stick plaatste, en aan de pers probeerde te lekken. Als de gegevens in de verkeerde handen terecht waren gekomen, had dit Boeing naar eigen zeggen tussen de 5 en 15 miljard dollar kunnen kosten.

*UBM Global: Ingeval van een vertrouwelijke informatielek via mobiele dragers moet forensisch onderzoek leiden tot informatie over wie er lekte, wanneer er is gelekt en welke vertrouwelijk informatie er is gelekt of zelfs is gestolen. De bewijslast ligt bij de organisatie.*

*DriveLock biedt deze gevraagde mogelijkheid. DriveLock maakt het eenvoudig voor systeembeheerders en onderzoekers om gebruikersactiviteiten te traceren. Een exclusieve applicatielog en uitgebreide event messaging geven de mogelijkheid om de informatie te krijgen over wat er in het netwerk en op de computers met randapparaten is gebeurd.*

*DriveLock 5.0 helpt daarmee ook in het bereiken van compliance met wet- en regelgeving, door auditmogelijkheden van alle administratieve acties zoals veranderingen aan white lists of aan toegangsrechten.*

*Om een organisatie tegen haar onwetende medewerkers te beschermen biedt DriveLock een inhoudsfilter. Deze filtert / blokkeert ongeautoriseerde via randapparaten inkomende en uitgaande bestand extensies of file typen, of inhoud van de bestanden.*

*Om de organisatie tegen haar wetende medewerkers te beschermen heeft DriveLock audit- en schaduwmogelijkheden:*

### *Auditing*

- *Logt acties met randapparaten*
- *Logt dataoverdracht, lees en schrijfactiviteiten van en naar verwijderbare opslagmedia en randapparaten met een schijf*
- *Heeft geavanceerde log mogelijkheden voor*
  - » *Configuratieveranderingen (inclusief veranderingsdetails)*
  - » *Gebruik management console*
  - » *Tijdelijke deblokkering van een agent*
  - » *Gebruik van agent remote control*
  - » *Encryptie events*
  - » *Opstarten of blokkeren van een applicatie*
  - » *Netwerkconfiguratie veranderingen*

### *Schaduw*

- *Een schaduwkopie kan worden gemaakt van alle bestanden van en naar verwijderbare opslagmedia en randapparaten met een schijf*
- *Limitering mogelijk tot de eerste paar regels van het bestand*
- *Uitsluiting mogelijk voor een lijst van file extensies*

*Indien een DriveLock licentienemer besluit om de schaduwfunctionaliteit te gaan gebruiken is het advies om eerst de ondernemingsraad en de werknemers te informeren.*

*De hierboven beschreven basisfunctionaliteiten van DriveLock, samengevoegd met de DriveLock Security Reporting Center (add on), maken forensische analyse heel eenvoudig.*

*Met DriveLock SRC is het nu mogelijk events te traceren tot aan de corresponderende white list entries (lijst met autorisatieregels). Voor verdere onderzoek en analyse met DriveLock SRC kunnen DriveLock events worden bekeken door gebruikmaking van flexibele filters met zoek- en groeperingcriteria. Vervolgens is er de mogelijkheid de resultaten te exporteren en te printen voor verdere analyse, verwerking, rapportage of bewijsvoering. Hierbij heeft de organisatie keuze uit een persoonlijk rapport met alleen toegang voor de huidige gebruiker, of een opgeslagen rapport met toegang voor andere gebruikers gebaseerd op configuratie instellingen overeenkomstig het informatieveiligheidsbeleid van de organisatie.*

*In alle gevallen kost het met DriveLock slechts enkele seconden om antwoorden te krijgen op forensisch vragen.*